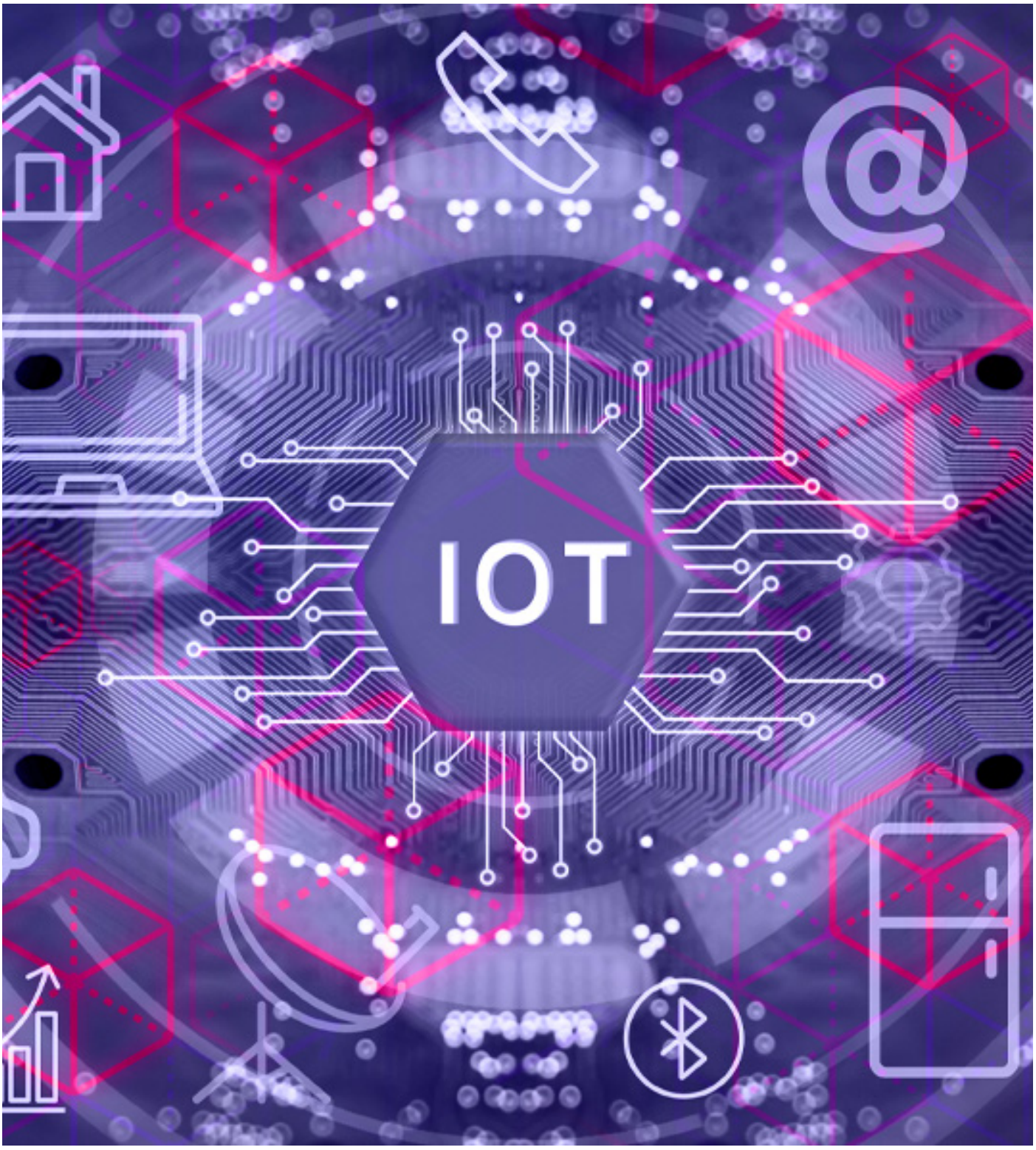
Mphasis
The Next Applied

Framework for Integration of Blockchain with IoT Devices

Whitepaper by Nidhi Agarwal
Group Manager, Business Process Management, Mphasis



Contents

1.

Introduction

Today's current IoT solutions depend on the centralized architecture by connecting to the cloud servers through the Internet. One of the drawbacks is that the widely expanded IoT-based infrastructure can create a single point of failure. More appropriate solutions need to be proposed, and this whitepaper gives an overview of a framework which will use blockchain, decentralized technology for the IoT device access control. The main benefits of the blockchain are great transparency, enhanced security, improved traceability, high efficiency, low costing and no third-party interference.

2.

Limitations of Current IoT Solutions

IoT cannot be fully trusted outside of data owner's sphere due to inability to verify that data is not manipulated before being sent, sold or used by third parties for their own benefits. For example, autonomous car startups and ride sharing giants such as Uber or Ola have no solution to share trusted mapping or ride data. Instead, they gather and store similar datasets independently in their servers.

Below are some of the limitations of current IoT solutions:

- Data integrity/ownership issues
- Highly centralized architectures
- Vulnerable to a variety of cyber-attacks
- Single point of failure
- Unattended environments

3.

How Blockchain can Address IoT Applications Limitation

A decentralized method to IoT networking would solve many of the problems mentioned above. Applying a reliable peer-to-peer communication model to process the trillions of transactions between devices will drastically reduce the costs related with installing and maintaining large, centralized data centers and will distribute computation and storage needs across the billions of devices that consist IoT networks. This will prevent failure in any single node in a network from bringing the entire network to a tentative collapse.

However, establishing peer-to-peer communications will present its own set of challenges, leading among them the issue of security. IoT security is much more than just about protecting sensitive data. The proposed framework will have to maintain privacy and security in huge IoT networks and offer some form of validation and consensus for transactions to prevent spoofing and theft.

To perform the functions of traditional IoT solutions without a centralized control, any decentralized approach must support three foundational tasks:

- Peer-to-peer messaging
- Distributed file sharing
- Autonomous device coordination

4.

Advantage of Blockchain for Integrating IoT Devices

Blockchain technology is the missing link to resolve privacy and reliability concerns on the IoT. Blockchain technology is the silver shot needed by the IoT industry. It can be used in tracking billions of connected devices, allowing the processing of transactions and harmonization between devices. This allows for significant savings for IoT industry creators. This decentralized approach would wipe out single points of failure, creating a more robust ecosystem for the devices. The cryptographic algorithms used by blockchains would make consumer data more confidential. The main advantages of the blockchain are great transparency, enhanced security, improved traceability, high efficiency, low costing and no third-party mediation. The combination of IoT enabled blockchain and well-designed incentives will be the catalysts to provide options in consumer data management.

Security needs to be built in as a base of IoT systems, with rigorous authority inspections, authentication, data verification and all the data needs to be encrypted. At the application level, software development organizations need to be better at implementing framework that is stable, resilient and trustworthy with better code development standards, training, threat analysis and testing. As systems work together with each other, it is essential to have an agreed interoperability standard, which is safe and valid. Without a solid bottom-top design, we will create more threats with every device added to the IoT. What is needed is a secure and safe IoT with privacy protected. That is a tough trade off, but not impossible and by defining a proper framework for blockchain-IoT technology application design and implementation and adherence to best practice is the key.

5.
Why Blockchain Based IoT Integrated Framework?

The blockchain IoT framework can:

- Obtain and manage data to create a standards-based, scalable and secure platform
- Integrate and secure data to reduce cost and complexity while safeguarding organization investment
- Analyze data and act by isolating business value from data, and then acting on it

The proposed framework for integrated IoT platform using blockchain technology:

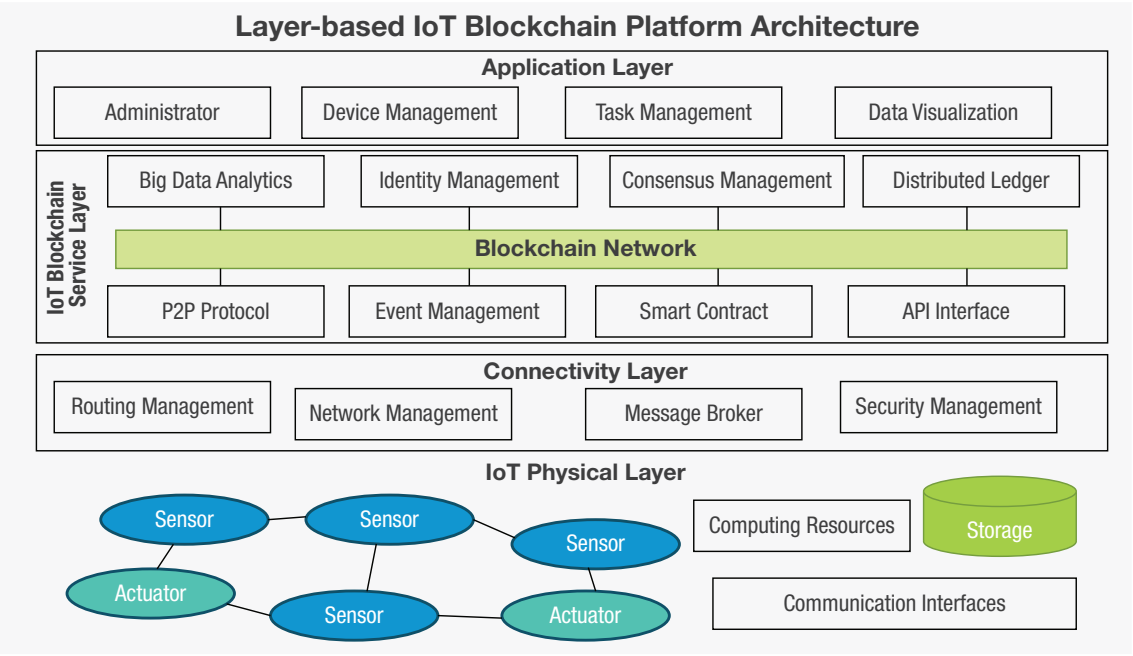
- Ensure sensing data integrity
- A practical application that provides a broad, immutable log and allows easy access to their devices deployed in different domains
- It provides features of general IoT systems, allows for real-time monitoring and control between the end user and device
- UI portal with – Login and workload management widgets (Case View, Task Lists)

6.
Suggested Architecture for IoT Blockchain Platform

6.1 Layered Architecture

Layered architecture is a modular architecture where each layer is decoupled from other layers so that the new module can be added or replaced without affecting the rest of the system.

6.1.1 IoT Physical Layer



The IoT physical layer consists of various associated devices with the capabilities of communication, computing and data storage.

6.1.2 Connectivity Layer

The main function provided by the connectivity layer is routing management because self-organization is needed since physical devices themselves have no global internet protocols (IPs).

This layer also includes other modules for providing below services:

- Network management
- Security management
- Message broker
- Routing management

6.1.3 The IoT Blockchain Layer

This service layer contains all modules that organize common services to provide various features of blockchain technologies like:

- Identity management
- Consensus
- Peer-to-peer (P2P) communication
- Distributed ledger

The distributed ledger is a consensus of replicated, shared and synchronized digital data that spread across the blockchain network, where network members owns the copy of the ledger. It provides safe storage space to record the device composition and sensing data provided by physical sensors. Any changes to the ledger are reflected in all copies in the blockchain network within seconds. The ledger can be either permissioned or permission less, regarding if anyone or only approved members can run a peer to validate transactions.

Big Data Analytics

The big data analytics module supports the blockchain to be an efficient mode for online data storage. Lots of transactional data from various parties are stored in structured forms of ledgers, which makes it an ideal source for further analysis. All these parties can be given access to one single network and can conveniently access these details.

Smart Contract

The smart contract is a business function invoked by an external client application to manage access and modifications in the ledger. It is installed and instantiated onto every peer of the network.

Event Management

The event management sends events every moment a new block is added to ledger or triggered whenever the predefined condition in the smart contract is completed.

API Interface

The API interface exposes the services provided by the blockchain network as services which can be invoked by the client application that can access and manage the network.

6.1.4 Application Layer

The top layer is the application layer, where various interfaces are required to visualize the data from physical devices, to manipulate and control devices.

6.2 Conceptual Architecture of the IoT Blockchain Platform

This architecture represents the conceptual scenario of the IoT blockchain platform, which consists of a massive number of IoT devices, user devices, data storages, local bridges and servers that are linked together around a peer-to-peer blockchain network.

6.2.1 IoT Server

The IoT server is a service provider that can interact with the local bridges and the blockchain network to provide a large variety of services for end users such as sending commands to perform some operations on the actuators, collecting sensing data from the bridge, querying data or storing data to the storage space via the blockchain network, etc.

6.2.2 Data Storage on Cloud

The data storage that belong to in the blockchain network can store environmental data collected by sensors, physical device profiles and device owner profiles. It can either be a software storage such as a DB or a hardware storage like a hard disk.

6.2.3 User Client

User client can be any terminal devices, such as smart phones, laptops and PCs through which end users can read or write data to the blockchain network.

6.2.4 Communication Protocols

There exists a wide choice of communication protocols for developers to apply on products and systems in IoT, such as Bluetooth®, ZigBee, WiFi and 2G-3G-4G cellular. Local bridges link a cluster of IoT devices to the server through these communication technologies and act as the service agent for these devices. With the evolution of hardware technology, embedded devices such as Raspberry Pi can directly consume web services by invoking representational state transfer application programming interfaces (REST APIs).

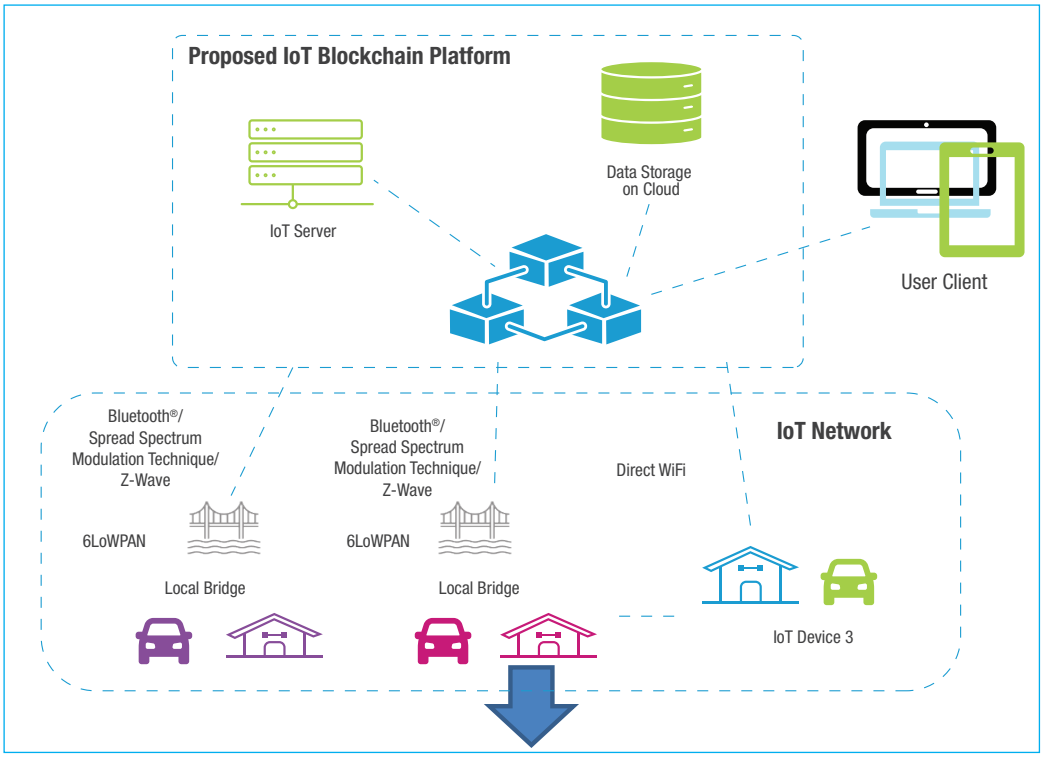
6.2.5 Communication Approach

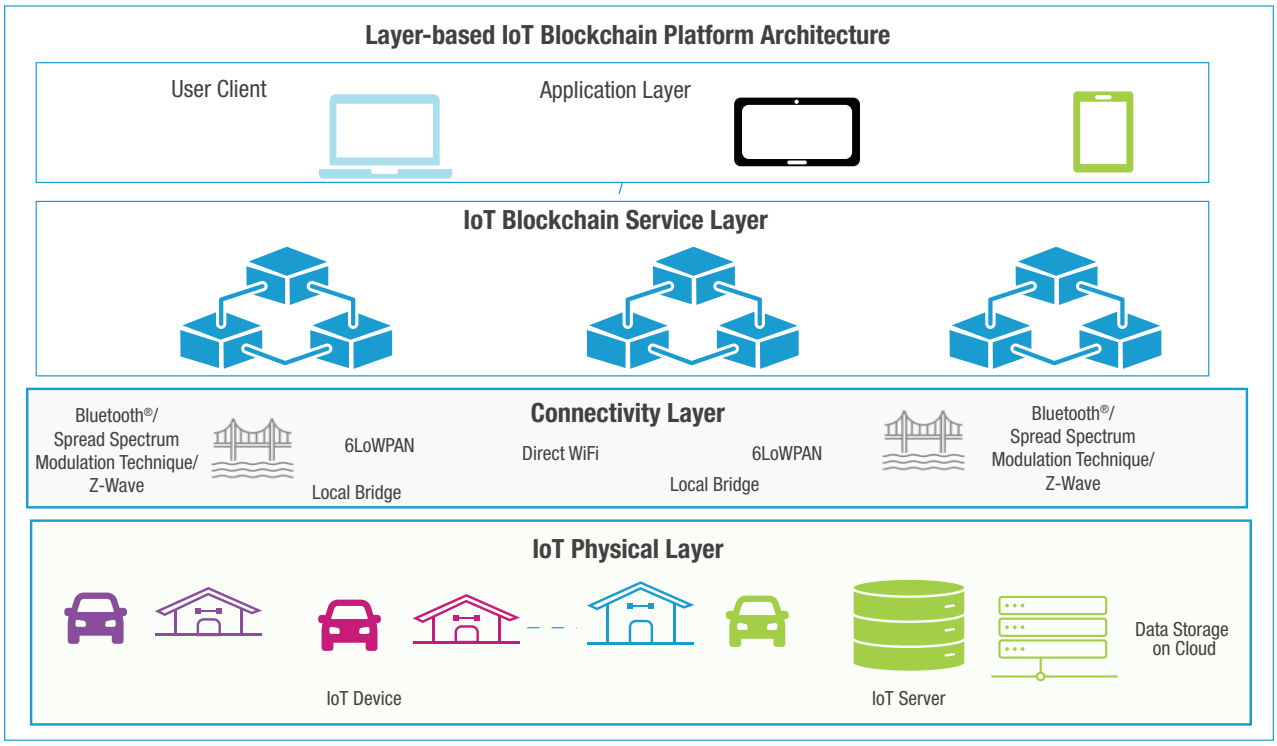
Two approaches are presented for communicating with physical devices, that is either via:

- The local bridges or
- Direct wireless communications

6.2.6 IoT Devices

The IoT devices can be classified into sensors and actuators: sensors are used to collect environmental data such as temperature and send these data to servers for further usage, while actuators are used to perform actions (e.g., turn on the light) according to commands received from end users.





7.
Applicability

Below are some of the use cases which can be explored for Blockchain – IoT application:

Car-sharing Services

The car-sharing market is relentlessly growing, and it has become even more popular than car ownership. Car-sharing system is centered on a centralized database server which can often lead to hacker attacks or password leaks. In car-sharing systems, the owners of the cars can exploit customers' data. As seen nowadays from a lot of use cases, the best solution to these challenging issues is to use blockchain technology. Blockchain as decentralized, immutable, public ledger provides the customers with security that is difficult to tamper.

Automotive Industry and Insurance

In the automotive industry, IoT is helping manufacturers make connected, autonomous, shared and electric vehicles a safe, practical experience. Insurers can use the data produced by these linked vehicles to monitor driving habits, develop personalized cover options and accurately process claims.

Retail Smart Homes

A host of smart household appliances and personal electronic devices will help to change the consumer goods industry transforming the user experience and providing retailers with a plethora of useful data.

Manufacturing

Manufacturers can create linked smart factories capable of monitoring equipment health, minimizing production costs and downtime, and maximizing productivity.

Smart Homes

Smart homes when powered by the blockchain framework technology, the IoT devices with virtual assistants will become much more proactive and secure.

8.

The Framework Proposed Brings the Advancements in IoT

8.1.1. Scalability

The proposed framework recommends the requirements of the practical IoT network which consists of several IoT devices connected through different restricted networks to a single blockchain network.

8.1.2. High Throughput

A high throughput network is needed to deal with synchronized communications among a large variety of devices. The framework proposes the use of a permissioned blockchain, in which interactions occur among a set of network entities that fully trust each. As a result, traditional voting-based protocols, like Byzantine Fault Tolerant (BFT) or Crash Fault Tolerant (CFT) consensus protocols are recommended to be used to improve the network throughput.

8.1.3. Lightweight

In the proposed framework, the IoT devices are not included in the blockchain, and a RESTful interface which will handle requests from devices is defined to enable cross platform communication between devices and the blockchain network.

8.1.4. Transparency

The suggested framework proposes a design that will hide the details of the IoT devices and the transaction history that records how a resource is manipulated, except for to the authorized user.

9.

Possible Value Realization

Blockchain can help lessen the security and scalability concerns associated with IoT in the following ways:

- The distributed ledger in a blockchain system is tamper-proof and this eliminates the need for trust among the involved parties. No single party has control over the massive amount of data generated by IoT devices.
- Utilizing blockchain to store IoT data would add another layer of security that hackers would need to bypass to gain access to the network. Blockchain provides a robust level of encryption that makes it virtually impossible to overwrite existing data records.

- Blockchain provides transparency only to authorized users to access the network to track the transactions that happened in the past. This can offer a reliable way to identify a specific source of any data leakages and take quick counteractive action.
- Blockchain can facilitate fast processing of transactions and coordination among billions of connected devices. As the number of interconnected devices grows, the distributed ledger technology provides a feasible solution to support the processing of the large number of transactions.
- By providing a way to enable trust among the stakeholders, blockchain can allow IoT companies to reduce their costs by eliminating the administering overheads related to IoT gateways like traditional protocol, hardware or communication overhead costs
- Smart contracts are an agreement between two parties that is stored in the blockchain and allow the execution of contractual arrangements among stakeholders based on certain criteria being fulfilled

To Realize the Business Benefits of the Framework:

- Build and adopt an ecosystem of IoT-enabled devices
- Select a use case
- Source, store and manage enormous amounts of data
- Adopt sophisticated analytics and machine learning capabilities
- Create new IoT applications that exploit data insights
- Choose a blockchain platform and setup environment
- Integrate IoT with blockchain and the blockchain into existing applications and workflows
- Deploy end-to-end security monitor and manage the entire value chain

10.
Designing the IoT Blockchain Platform with a Sample Use Case

Car-sharing services use case is considered to demonstrate how we can utilize the framework.

10.1 Detailed Use Case Mapping

The aim of the proposed solution is to design peer-to-peer short term car-sharing application based on blockchain technology and smart contracts. For the implementation of smart contracts, Hyperledger Fabric framework is used. The key objective is to design a peer-to-peer car-sharing service solution without a central authority which will decrease the costs and increase the data

transparency in that system. The framework recommends the token-based solution that gives us ability to cover business-to-business (B2B) and business-to-customer (B2C) use cases. Smart contracts of Hyperledger operate on the Internet of Things (IoT) and control a new decentralized version of the sharing economy for use case sharing services like Uber and Airbnb that operate in peer-to-peer mode without centralized management. Smart contracts represent a disruptive novelty with a huge potential.

10.2 Blockchain Platforms to be Considered for Creating IoT Blockchain Applications

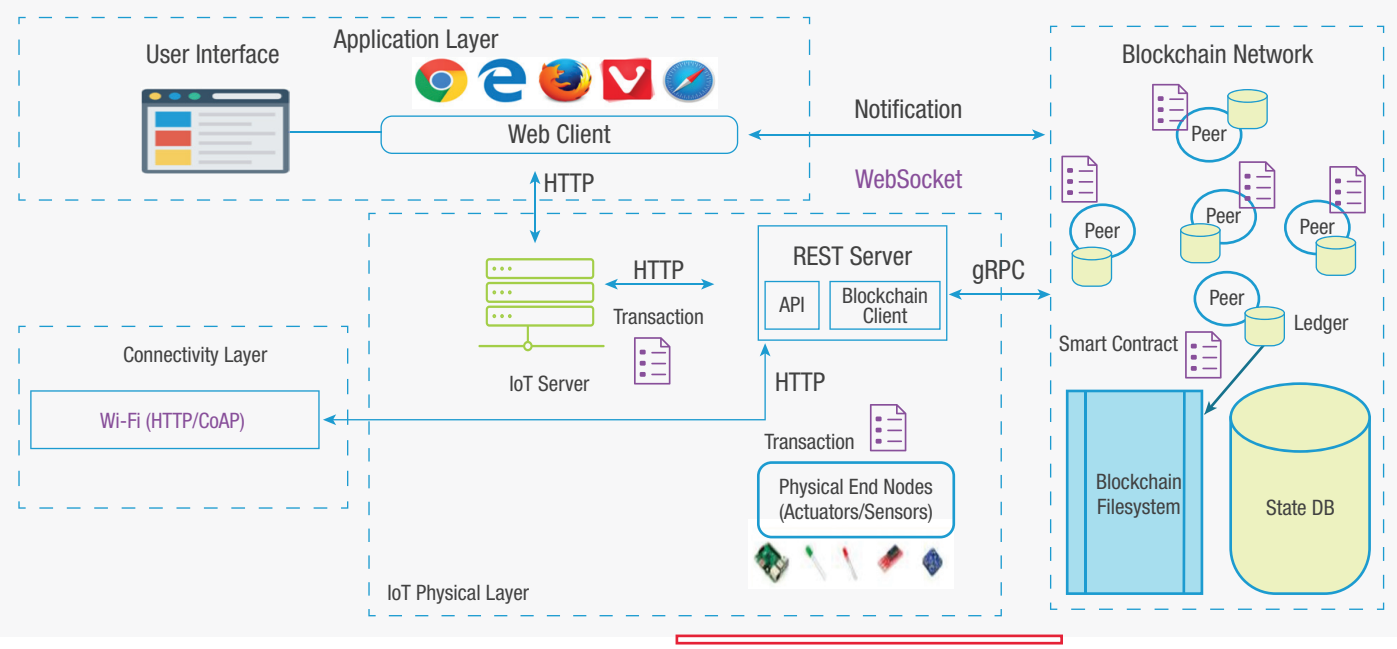
The number of blockchain platforms is so high and in constant change that it is impossible to analyze them all so in this table we have listed the most popular and suitable for IoT domains.

Blockchain	Mode of Operation	Consensus	Crypto Currency	Smart Contract
Ethereum	Public and Permission-based	PoS	Ether (ETH)	Yes
Hyperledger Fabric	Permission-based	PBTF/SIEVE	None	Yes
MultiChain	Permission-based	PBTF/SIEVE	Multi-currency	Yes
Litecoin	Public	Scrypt	Litecoins (LTC)	No
Lisk	Public and Permission-based	DPoS	LSK	Yes
Quorum	Permission-based	Multiple	ETH	Yes
HDAC	Permission-based	ePoW, Trust-based	Multi-asset	Yes

10.3 IoT Devices to be Used in Blockchain Applications

Source	IoT Device	Mode	Blockchain
EthEmbedded	Raspberry Pi, BeagleBone Black, Odroid XU3/XU4, Wandboard, Ethcore Parity	Full node	Ethereum
Ethraspbian	Raspberry Pi, BeagleBone Black, Odroid XU3/XU4, Wandboard, Ethcore Parity	Full node	Ethereum
Raspnode	Raspberry Pi	Light node	Hyperledger Fabric
Bitmain	Antrouter R1-LTC	Full node miner	Litecoin

10.4 Designing the Blockchain-IoT Application



This diagram represents the implementation environment for designing the car-sharing use case, and also presents the means of connection between the IoT devices, the server and the blockchain network.

- The IoT device server is hosted on the Raspberry Pi, which is integrated with various physical sensors and actuators
- Hyperledger Fabric framework is used to construct the blockchain network where four peers and an orderer node are running as images in the docker container
- Each peer contains the smart contract and data storage to write a block of transactions to the ledger
- Couch DB is used as the state database that provides rich query support and the smart contract data is modeled as JavaScript Object Notation (JSON). It supports various query methods such as get, put and delete in conjunction with a state key, which enables the application to invoke a smart contract to access world states through simple APIs.
  In contrast to the state database, the blockchain is physically implemented in a file, as the blockchain data structure is always used to record a limited small set of simple operations.
- The REST server provides various RESTful APIs that expose the functions specified by the blockchain network. All these services can be invoked by either a web client or a physical device directly.
- It also hosts the Fabric client, which utilizes Google remote procedures calls (gRPC) system to communicate with the Hyperledger Fabric network
- The blockchain acts as a transaction log that records all the state changes

- Transactions are collected into blocks that are cryptographically linked together to form a sequence of chains, where all transactions on the ledger are sorted in time order, enabling the user to know the history modifications that happened in the state database. The orderer node is employed with the PBFT algorithm to ensure the consistency of every copy of the ledger.
- This node exists independently of the peer processes and orders transactions on a first-come-first-serve basis across the network
- The notification generated from the blockchain network is emitted to the client using WebSockets

11.

Conclusion - The Expected Product Outcome from this Framework

The centralized architecture like the cloud model can have high costs, latency and the risk of single point of failure. Blockchain technologies offer a new security protocol and infrastructure to allow billions of IoT devices to have trusted interoperability for both data and commerce. This paper outlines an approach for the framework of a decentralized IoT platform to address scalability, identity and data security challenges based on a blockchain network.

Companies should start considering the implementation of blockchain and IoT to address their business issues, ‘starting small’ by learning from current use cases and using the right framework to design and implement the blockchain and IoT application.

The Blockchain-IoT Framework Suggests Building the Application Right Way

- Select the most suitable blockchain platforms for creating IoT Blockchain Application
- Select the relevant IoT devices to be used in blockchain applications
- Design and implement the blockchain-IoT application in the most appropriate way

11.1 Scenario 1

For scenario 1, we will need:

- IoT device with full/lite blockchain node
- Web UI or mobile app with Web3.js Library
- Web 3 provider-smart contract using Web 3 Library
- Blockchain network

11.2 Scenario 2

For scenario 2, we will need:

- IoT device without blockchain software
- Gateway device with blockchain node and data aggregation
- Web UI or mobile app with Web3.js Library
- Web 3 provider-smart contract using Web 3 Library
- Blockchain network

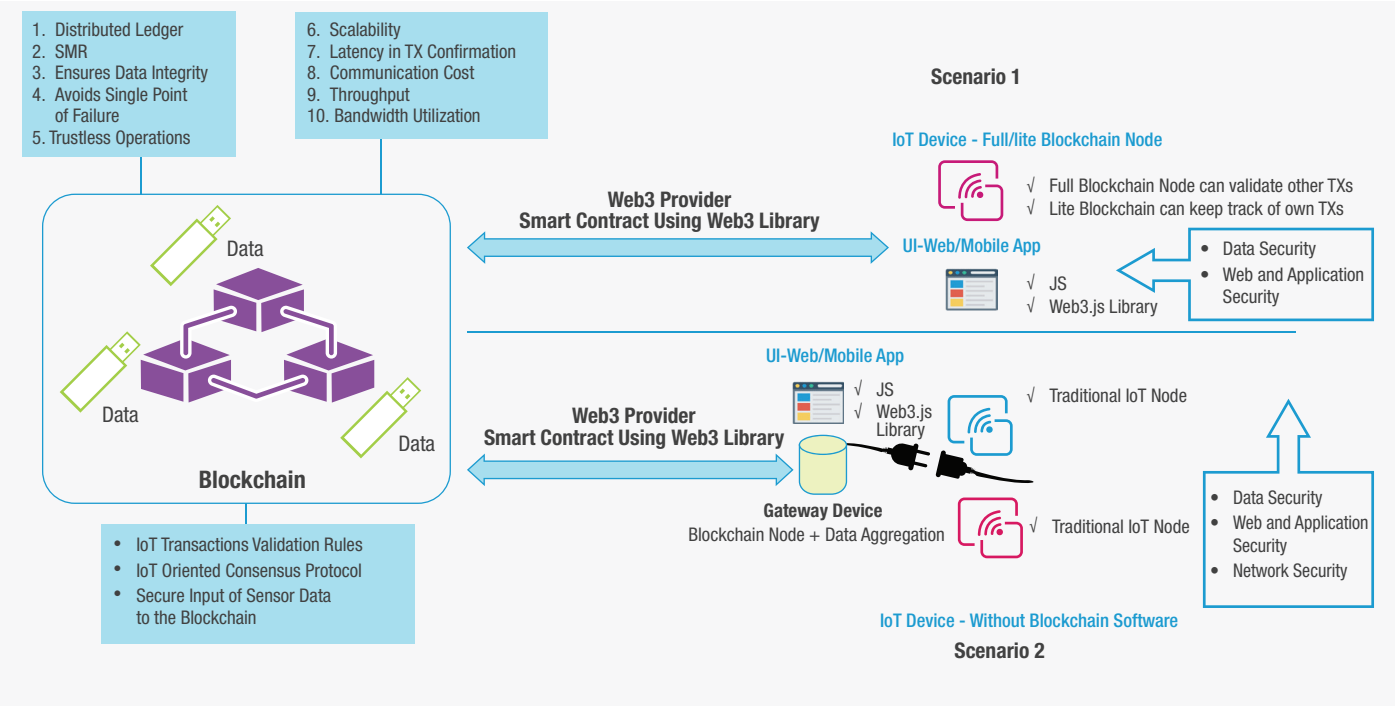


Figure Depicting Scenario 1 and Scenario 2

Author

Nidhi Agarwal

Group Manager, Business Process Management, Mphasis

Nidhi Agarwal is Group Manager, Business Process Management (BPM) at Mphasis and comes with 17+ years of IT experience spanning BPM practice leadership, project and program management, service delivery, development and consulting. Nidhi manages Pre Sales, Go To Market, Account Mining, Alliances, Collateral Starter Kits and Knowledge Management for the BPM Practice. She is also responsible for New Logo Wins, generating revenues from IP/solutions/T&A, and operational responsibilities include Revenue Forecasting, Bench Management, etc. On the technology and skills front, Nidhi is proficient in Pega, Appian, Camunda, IBM BPM and holds a Postgraduate Diploma in Blockchain from Amity University. She is trained in Robotic Process Automation (RPA) and Robotic Desktop Automation (RDA), Microsoft Visio, Scrum & Agile methodologies, BPM product evaluation, DevOps, Docker and Testing Based Development.

About Mphasis

Mphasis (BSE: 526299; NSE: MPHASIS) applies next-generation technology to help enterprises transform businesses globally. Customer centricity is foundational to Mphasis and is reflected in the Mphasis' Front2Back™ Transformation approach. Front2Back™ uses the exponential power of cloud and cognitive to provide hyper-personalized ($C = X2C^{2}_{TM} = 1$) digital experience to clients and their end customers. Mphasis' Service Transformation approach helps 'shrink the core' through the application of digital technologies across legacy environments within an enterprise, enabling businesses to stay ahead in a changing world. Mphasis' core reference architectures and tools, speed and innovation with domain expertise and specialization are key to building strong relationships with marquee clients. To know more, please visit www.mphasis.com

For more information, contact: marketinginfo.m@mphasis.com

USA
460 Park Avenue South
Suite #1101
New York, NY 10016, USA
Tel.: +1 212 686 6655

UK
1 Ropemaker Street, London
EC2Y 9HT, United Kingdom
T : +44 020 7153 1327

INDIA
Bagmane World Technology Center
Marathahalli Ring Road
Doddanakundhi Village
Mahadevapura
Bangalore 560 048, India
Tel.: +91 80 3352 5000

www.mphasis.com

NR 02/03/21 US LETTER BAS1167S0